## What is claimed is:

**[Claim 1]** A process for protecting the characteristics of a transaction accessing assets in an account or information corresponding to an account, either held by an account custodian, including a credit card account, comprising the steps of: mapping at least one identification code to at least one diversionary identification code; storing said mapping on an intercept system, said intercept system connected to said network and including data storage and a computer system; when said diversionary identification code is entered into an access device, said diversionary identification code instructs said access device to route the access transaction to said intercept system; when said access transaction is routed to said intercept system, said intercept system compares at least one diversionary identification code to said mapping; wherein if said mapping indicates that said access transaction meets a masking criteria, said access transaction will be processed through said intercept system according to a set of masking instructions, wherein said masking instructions include contacting said account custodian via a network with masked transaction information.

**[Claim 2]** The process for protecting the characteristics of a transaction as recited in claim 1, wherein said at least one identification code includes at least a portion of the information included on the encoded magnetic stripe of a card used in financial transactions.

**[Claim 3]** The process for protecting the characteristics of a transaction as recited in claim 1, wherein said masking instructions include processing said transaction according to any instructions processed at said access device.

**[Claim 4]** The process for protecting the characteristics of a transaction as recited in claim 3, wherein said account custodian will record said intercept system as said access device.

**[Claim 5]** The process for protecting the characteristics of a transaction as recited in claim 3, wherein said intercept device has a plurality of locations.

**[Claim 6]** The process for protecting the characteristics of a transaction as recited in claim 3, wherein said intercept device records said instructions from said access device in an encoded form.

**[Claim 7]** The process for protecting the characteristics of a transaction as recited in claim 6, wherein said encoded transactions may be decoded only by a password supplied to an account holder.

**[Claim 8]** The process for protecting the characteristics of a transaction as recited in claim 3, wherein said access device is a POS terminal for a credit card.

**[Claim 9]** A system for protecting the identity of a transaction conducted at least partially over a network, including: a replacement transaction device in the form of a card with data at least corresponding to account information and a contingency transaction identifier; a proxy transaction system connected to said network including a proxy transaction server; wherein when said replacement transaction device is used, said proxy transaction server is activated, said proxy transaction server contacts an account custodian over a network in order to process said transaction; wherein said transaction is only known via said network to said account custodian through said proxy transaction system.

**[Claim 10]** A method for protecting user information available over a network and physically located in electronic storage with an account custodian, wherein said user information is accessed by at least entering into an access device, a first security identifier known and entered by a user, including the acts of: providing said user with a second security identifier, said second security identifier distinguishable from said first security identifier; when said second security identifier is entered into said network and detected by said account custodian, said account custodian provides access to alternate information, said alternate information distinguished from said user information, whereby it would not be apparent to an observer other than said user that said alternate information is not said user information.

**[Claim 11]** The method as recited in claim 10, wherein said alternate information is a non-secure subset of said user information.

**[Claim 12]** The method as recited in claim 10, wherein said alternate information is fictitious.

**[Claim 13]** The method as recited in claim 10, wherein said access is provided over a WAN.

**[Claim 14]** The method as recited in claim 10, wherein said user information is personal information.

**[Claim 15]** The method as recited in claim 10, wherein said alternate information is transactional information.

**[Claim 16]** The method as recited in claim 15, wherein said transactional information is fictitious and related to the geographical origin of said transaction.

**[Claim 17]** The method as recited in claim 15, wherein said transactional information is fictitious and related to an account number.

**[Claim 18]** The method as recited in claim 15, wherein said transactional information is fictitious and relates an account balance.

**[Claim 19]** The method as recited in claim 18, wherein said account balance is fictitiously low.

**[Claim 20]** The method as recited in claim 18, wherein said account balance is fictitiously high.